Address Resolution Protocol (ARP), The Network Layer and Routing concepts

Outline

This unit will help to understand the concept of Address Resolution Protocol (ARP) and how it works to allow for successful communication. We will also learn about the purpose and characteristics of the network layer, routing protocols and the routing table.

Learning Outcomes

- Distinguish among the binary, hexadecimal and decimal numbering systems.
- Describe the ARP process and examine the ARP table.
- Describe the characteristics of the network layer.
- Explain how routing decisions are made with the help of a routing table.
- Configure static routes.
- Differentiate among the different types of routing protocols.

In-class activity on Address Resolution Protocol (ARP)

Let us discover how ARP works by watching the video available at the below link:

https://youtu.be/b_x7vyE4wtc

Week 5: In-class Packet Tracer Lab on ARP

Create a topology on Cisco Packet Tracer consisting of 3 PCs (PC0 - PC2) connected to a central switch with the below addressing scheme.

Addressing scheme and connections

Device	IP address	Subnet Mask	Connected to switch port
PC0	10.10.10.1	255.255.255.0	Fa0/0
PC1	10.10.10.2	255.255.255.0	Fa0/1
PC2	10.10.10.2	255.255.255.0	Fa0/2

Switch to simulation mode and observe what happens when a ping is launched from PC0 to PC1. Click Capture/Forward until the ICMP reply is received by PC0.

Week 5 & 6: In-class presentation on The Network Layer and Routing Concepts

Network Layer charateristics

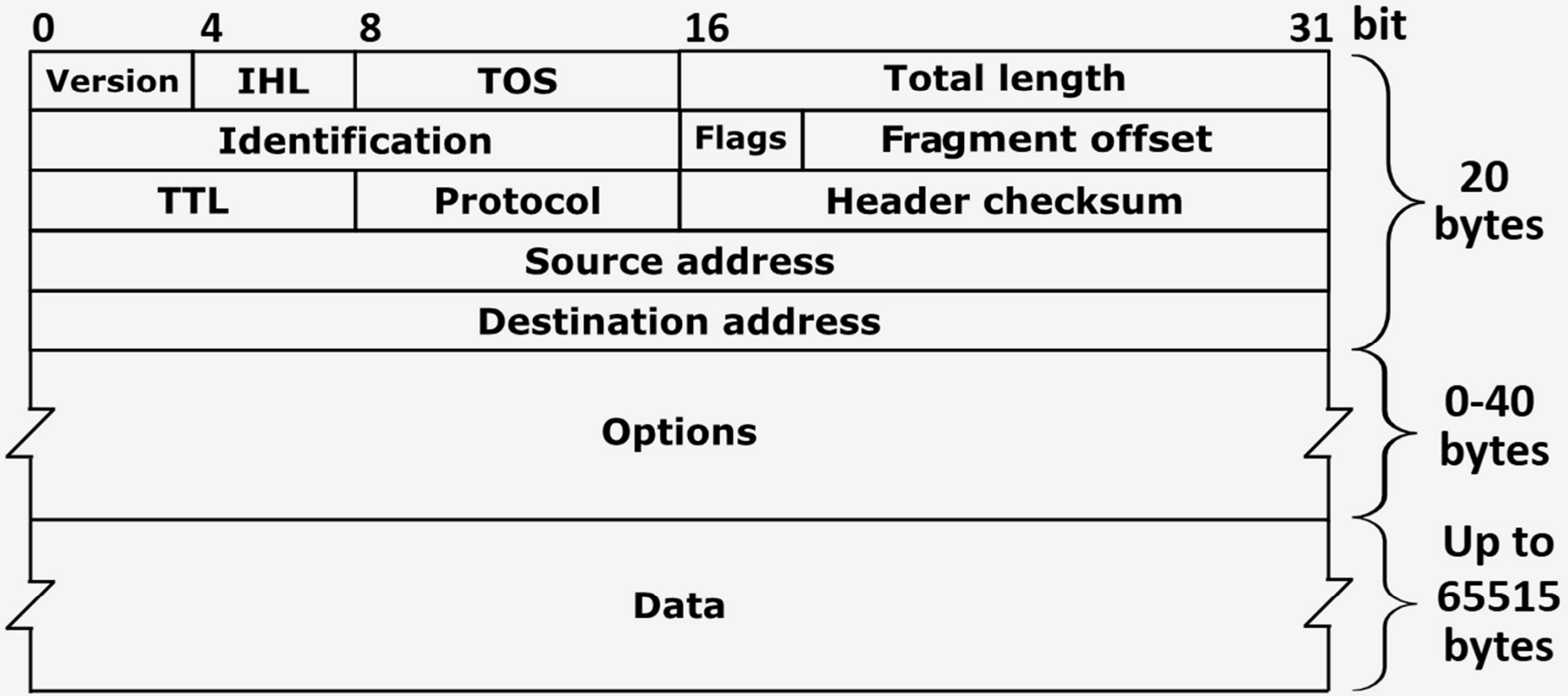
The main task of the network layer is to get packets from any one node in the network to any other node.

There is one predominant network layer protocol which is the “Internet Protocol”, or IP.

There are four basic operations that are accomplished by the network layer:

1. Addressing of end devices (IP addressing / logical addressing)
2. Routing: Routing is the global decision of how a packet should go from its source to its final destination.
3. Encapsulation
4. De-encapsulation

IPv4 Packet



IPv4 Packet fields

The many fields are described below:

- Which version of IP is this packet for?
- The number of bytes of the IP header. There are options which may be included, so the size can vary. Normally there are no options, and the header is 20 bytes.
- Type of service bits allow for networks to prioritize certain types of communication, for example real-time voice data might prioritized over email packets.
- The data length is how many bytes of data are included in the packet. They usually are no larger than 1500 bytes, so they can fit into an Ethernet frame.
- The identifier, flags and fragment offset deal with packet fragmentation. It is possible that an IP packet will be broken into multiple link layer frames. These fields allow the router receiving the frames to re-assemble them into 1 complete packet.

IPv4 Packet fields (Cont'd)

- The time to live field is to prevent packets from cycling around the network endlessly. This field is an integer which is decremented each time the packet is forwarded. If the value reaches 0, the packet will be dropped instead of forwarded further. The initial value is often 64.
- The upper layer protocol field distinguishes what sort of data is contained, this is principally TCP or UDP.
- The header checksum contains a checksum on the header information, so the data can be verified by the receiver.
- The source and destination IP addresses are the initial source node and final destination node of the packet.
- Options are not normally included, they include things like specifying routing parameters, and experimental routing options. Many routers block these even if they are included.
- Finally the data is the TCP or UDP packet that the IP layer is meant to be sending.

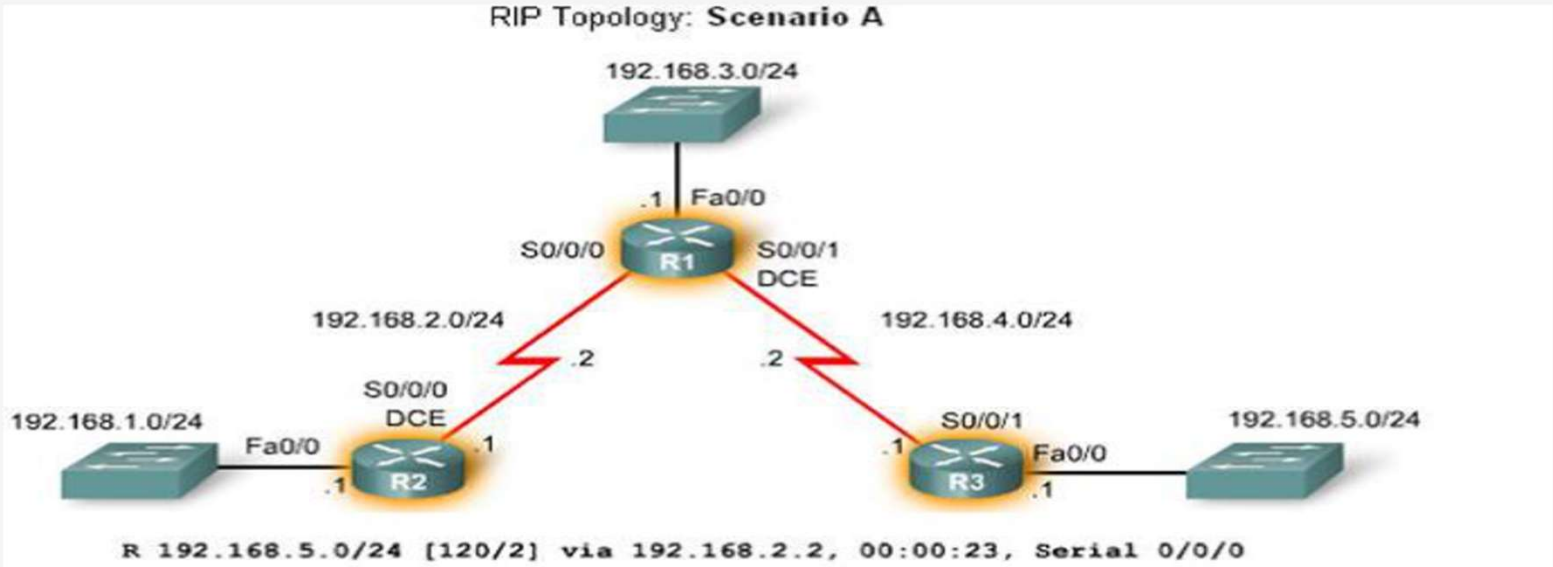
Routers

Routers implement layer 3 or network layer functions. Their main job is to forward packets based upon a routing table.

The basic routing function can be split into two areas; one is to build a map of the network and secondly to forward the packets.

To build the map, routers typically use either static routing or dynamic routing protocols. With the help of dynamic routing protocols, routers will let other network devices know about not only the topology of the network but also about network changes. Static routing will be that static and will not adapt to network changes. Both models accomplish the task of building the map of the network in the form of the routing table.

With show IP route, an IOS Cisco device shows the different destinations, the metric to get there, the administrative distance to define priorities for different routing protocols, and the next-hop to get to that destination.



Interpreting a RIP Route in the Routing Table

R	Identifies the source of the route as RIP.
192.168.5.0	Indicates the address of the remote network.
/24	The subnet mask used for this network
[120/2]	The administrative distance (120) and the metric (2 hops)
via 192.168.2.2	Specifies the address of the next-hop router (R2) to send traffic to for the remote network.
00:00:23	Specifies the amount of time since the route was updated (here, 23 seconds). Another update is due in 7 seconds.
Serial0/0/0	192.168.2.2

Default Gateway

A host routes to the default gateway.

A router or layer 3 switch can be a default-gateway.
Features of a default gateway (DGW):

- It must have an IP address in the same range as the rest of the LAN.
- It can accept data from the LAN and is capable of forwarding traffic off of the LAN.
- It can route to other networks.

If a device has no default gateway or a bad default gateway, its traffic will not be able to leave the LAN.

Routing Table

The routing table contains the network layer intelligence that tells the router how to forward packets to remote destinations.

Initially, that routing table is made up of networks that are directly connected to the particular router.

They are shown as directly connected networks (with code **C**), after that the way to learn about remote destinations is by either populating the routing table with static routes in which an administrator will tell the router how to get to the destination or by populating the routing table via routing table advertisements coming from other routers.

For remote networks, code is **S** for static routes or **O** (for OSPF) / **D** (for EIGRP) / **R** (for RIP) depending on the routing protocol configured.

A default route might also be present represented as 0.0.0.0/0 for destination networks that are not explicitly present in the routing table.

Static routing

Static routing consists of individual configuration commands that define a route to a router.

A router can forward packets only to subnets in its routing table.

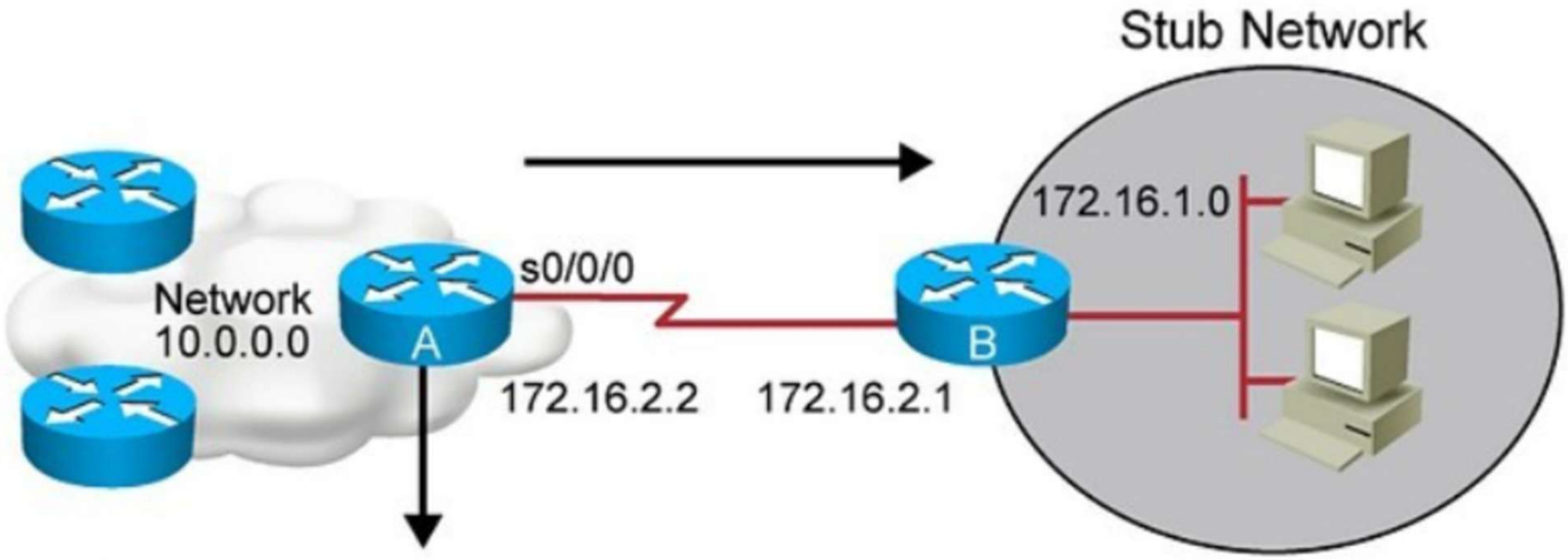
The router always knows about directly connected routes-routes to subnets off interfaces that have an “up and up” status.

By adding static routes, a router can be told how to forward packets to subnets that are not attached to it.

In order to configure static routing in Cisco IOS routers, this is the command to use.

```
Router(config)#ip route [network/host] [mask] [address/interface]
```

Here is an example of a static route configured at router A there.




```
RouterX(config)# ip route 172.16.1.0 255.255.255.0 172.16.2.1
```


or

```
Router(config)#ip route 172.16.1.0 255.255.255.0 s0/0/0
```

What is a Dynamic Routing Protocol?

Routing protocols define the rules for the dynamic exchange of information between routers to build the routing table for a routed protocol.

The routed protocol will then use that information to drive the packets and find the best path to a destination.

So the routing protocols are like the builders of a map to a city and then the routed protocol is the one driving the packets using the information from the map to go around the city.

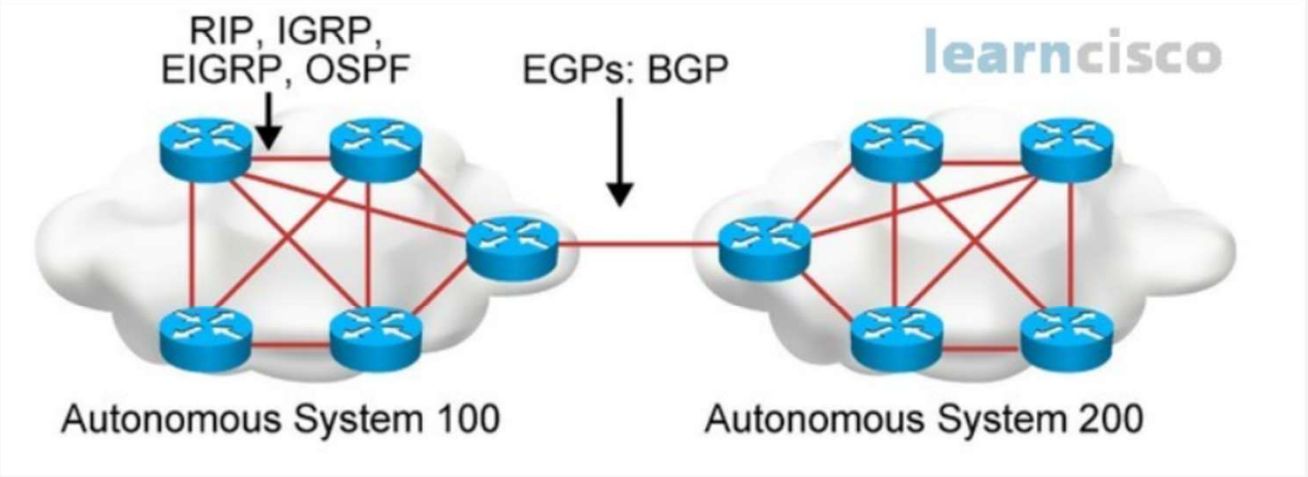
The analogy is complete if you think of the builders of the map adjusting continuously to changes in terms of new streets, streets that may be blocked or no longer available.

In understanding how routing protocols work, we need to understand the context in which they work. One first way to classify them could be as exterior gateway protocols or interior gateway protocols.

Autonomous Systems: Interior or Exterior Routing Protocols

Interior gateway protocols (IGP) will be those routing protocols working inside of an autonomous system. Exterior gateway protocols (EGP) are those connecting or working between autonomous systems.

An autonomous system is a collection of networks under a common administration and sharing a common routing strategy and policies. So it is common to see a set of routing protocols working or configured as part of an organization's networks, even if that organization spans across multiple geographic areas.



Autonomous Systems: Interior or Exterior Routing Protocols (Cont'd)

The concept is more of an administration scope and not necessarily a geographic scope.

You could have a WAN between two networks but if those two networks are maintained by the same administration team under the same routing policies and belonging to the same organization, then those routing protocols are interior.

In real life, the concept of an autonomous system is very much related to the Internet. All networks connected to the Internet will either have their own autonomous system number or will belong to their service provider's autonomous system.

In that sense, the only exterior gateway protocol is BGP, which is a routing protocol we speak out in the Internet.

The others there are considered interior gateway protocols and are typically run within the confines of an organization's private networks.

Week 6: In-class Packet Tracer Lab on Router Initial configuration and static routes

Research on the basic initial configurations that need to be added on a router and configure same on Packet Tracer. A class discussion will then follow to ensure that everyone configured the main basic configurations as required.

We will then discuss as a group about the number of static routes that need to be added for the below topology and I will demonstrate the configuration on Packet Tracer.